The D/SPBS, may revisit the matter with the Senior Agency Official or refer the matter to the Security Policy Forum as deemed appropriate.

(D) Should the matter remain unresolved, the Security Policy Forum may consider referral to the SPB, the agency head, or the National Security Council as deemed appropriate.

(ii) *Industry*. (A) Contractor employees are encouraged to bring suspected departures from the reciprocity provisions of the NISPOM to the attention to their Facility Security Officer (FSO) or Contractor Special Security Officer (CSSO), as appropriate, for resolution.

(B) Should the matter remain unresolved, the complainant (employee, FSO, or CSSO) is encouraged to report the matter formally to the Cognizant Security Office (CSO) for resolution.

(C) Should the CSO responses be determined inadequate by the complainant, the matter should be reported formally to the Senior Agency Official within the Cognizant Security Agency (CSA) for resolution.

(D) Should the Senior Agency Official response be determined inadequately by the complainant, the matter should be reported formally to the Director, information Security Oversight Office (ISOO) for resolution.

(E) The Director, ISOO, may revisit the matter with the Senior Agency Official or refer the matter to the agency head or the National Security Council as deemed appropriate.

(2) An annual survey administered to a representative sampling of agency and private sector facilities to assess overall effectiveness of agency adherence to applicable reciprocity requirements.

(i) In coordination with the D/SPBS, the Director, ISOO, as Chairman of the NISP Policy Advisory Committee (NISPPAC), shall develop and administer an annual survey to a representative number of cleared contractor activities/employees to assess the effectiveness of interagency reciprocity implementation. Administration of the survey shall be coordinated fully with each affected Senior Agency Official.

(ii) In coordination with the NISPPAC, the D/SPBS shall develop and administer an annual survey to a representative number of agency activities/personnel to assess the effectiveness of interagency reciprocity implementation. Administration of the survey shall be coordinated fully with each affected Senior Agency Official.

(iii) The goal of annual surveys should not be punitive but educational. All agencies and departments have participated in the crafting of these facilities policies, therefore, non-compliance is a matter of internal education and direction.

(e) Agencies will continue to review and assess the potential value added to the process of co-use of facilities by development of electronic data retrieval across government.

PART 149—POLICY ON TECHNICAL SURVEILLANCE COUNTERMEASURES

Sec.
149.1 Policy.
149.2 Responsibilities.
149.3 Definitions.

AUTHORITY: E.O. 12968 (60 FR 40245, 3 CFR 1995 Comp., p. 391.)

SOURCE: 63 FR 4583, Jan. 30, 1998, unless otherwise noted.

§ 149.1 Policy.

(a) Heads of federal departments and agencies which process, discuss, and/or store classified national security information, restricted data, and sensitive but unclassified information, shall, in response to specific threat data and based on risk management principles, determine the need for Technical Surveillance Countermeasures (TSCM).

To obtain maximum effectiveness by the most economical means in the various TSCM programs, departments and agencies shall exchange technical information freely; coordinate programs; practice reciprocity; and participate in consolidated programs, when appropriate.

§ 149.2 Responsibilities.

(a) Heads of U.S. Government departments and agencies which plan, implement, and manage TSCM programs shall:

(1) Provide TSCM support consisting of procedures and countermeasures determined to be appropriate for the facility, consistent with risk management principles.